FortiConverter v4.3.0

Release Notes

FortiConverter v4.3.0 Release Notes

January 15, 2014

33-420-0217152-20140124

Technical Documentation	docs.fortinet.com
Feedback and Support	fconvert_feedback@fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Introduction

FortiConverter provides a solution for the conversion of numerous firewall configurations into a FortiOS-compatible format. Support is currently provided for Cisco, Check Point, Juniper and SonicWall conversions. A trial version is available, which allows for some functional testing to be performed before purchase. This trial version is limited in overall functionality but should prove sufficient for initial product evaluation.

SKU	Description
FC-10-CON01-401-01-12	1-Year Multi-vendor Configuration Conversion Tool (requires MS Windows) to create FortiOS configuration files.
FC-10-CON01-401-02-12	1-Year Renewal Multi-vendor Configuration Conversion Tool (requires MS Windows) to create FortiOS configuration files.

New Features

FortiConverter 4.3 adds the following new features:-

- Direct conversion from Check Point Provider-1 to FortiManager
- Conversion of Snort rules to FortiOS custom IPS signatures
- Cisco ASA Object NAT and Twice NAT conversion

Enhancements

- NAT Tuning improvement to meet different vendor approaches
- Tool tip for NAT objects for improved clarity
- 'In progress' status improvement to show current conversion activity
- Over-length objects reduced to comply with FortiOS requirements
- Report for unconverted objects for both Cisco and Check Point
- For trial users if the final FortiGate file contains more than 100 lines of configuration, the GUI will allow for browsing of this configuration. A complete configuration is not provided for trial users.

System Requirements

FortiConverter is designed to run on the following MS Windows platforms:-

- Microsoft Windows 8 (32/64 bit)
- Microsoft Windows 7 (32/64 bit)
- Microsoft Windows Vista (32/64 bit)
- Microsoft Windows XP (32 bit)

Supported Vendors

Firewall configurations are supported from the following vendors:-

Check Point

Smart Center with OS NG FP1 (4.0) to NGX R76

Provider-1 with OS NGX R65 to R76

Juniper

SSG ScreenOS 5.x / 6.x

SRX JunOS 10.x, / 11.x / 12.x

Cisco PIX/ASA/FWSM

PIX: 5.x / 6.x / 7.x / 8.x

ASA: 7.x / 8.x

FWSM: 2.x / 3.x / 4.x

Cisco IOS

OS: 10.x / 11.x / 12.x / 15.x

SonicWall NSA

OS: SonicOS Enhanced 5.x

Supported Conversions

Check Point

Interface (physical, logical, loopback, PPPoE)
Addresses / address group
Service / service group
Schedules
Rule
NAT (automatic NAT / rule NAT)
VPN (IPsec)
Local user / user group
AAA server (RADIUS / TACACS+ / LDAP)
Static route

Juniper

Interface (physical, logical, loopback, PPPoE, tunnel)
Zone
DHCP server / client / relay
Policy

NAT
Address / address group / FQDN
IP pool
VIP / MIP
Service/service group
Static routes
VPN (IPSEC, PPTP / L2TP)
Local user / user group

Cisco

Interface (physical, logical, loopback, PPPoE, tunnel)
Address / address group
IP pool
Time-range
DHCP server
Service / service group
Static routes
ACL
NAT
VPN (IPSEC, PPTP / L2TP)
Local user / user group
AAA server (Radius / TACACS+/LDAP)

Sonicwall NSA

Interface (physical, logical, loopback, PPPoE)
Zone
DHCP server / client / relay
Policy
NAT
Address/ address group
Services/ service group
Static routes
Schedule
Local user / user group

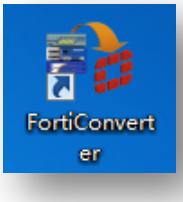
Installation

The following instructions will guide you through the installation of FortiConverter

The Microsoft .NET framework is required by FortiConverter. If this is not already available you will be prompted to install this via the Microsoft website.

1. Double-click the FortiConvertertSetup executable file to launch the setup wizard. The *Setup Wizard* will install FortiConverter on your computer.

2. After accepting the license agreement and selecting an install location, FortiConverter will be ready for use. Double-click the desktop shortcut icon.



Activating the Full Version

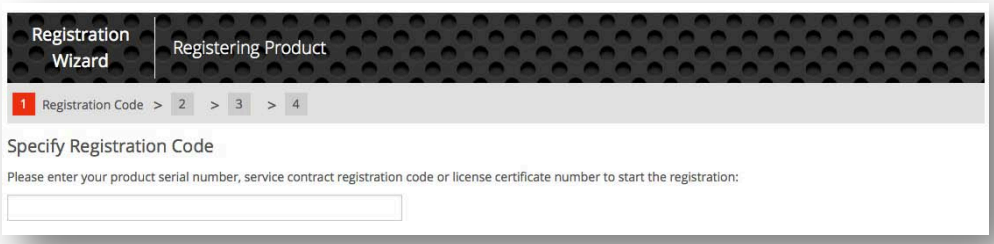
When first installed, FortiConverter has a temporary, restricted trial license. If you have purchased a full license, this will need to be separately installed to unlock the full product functionality.

1. From the main panel select License Activation

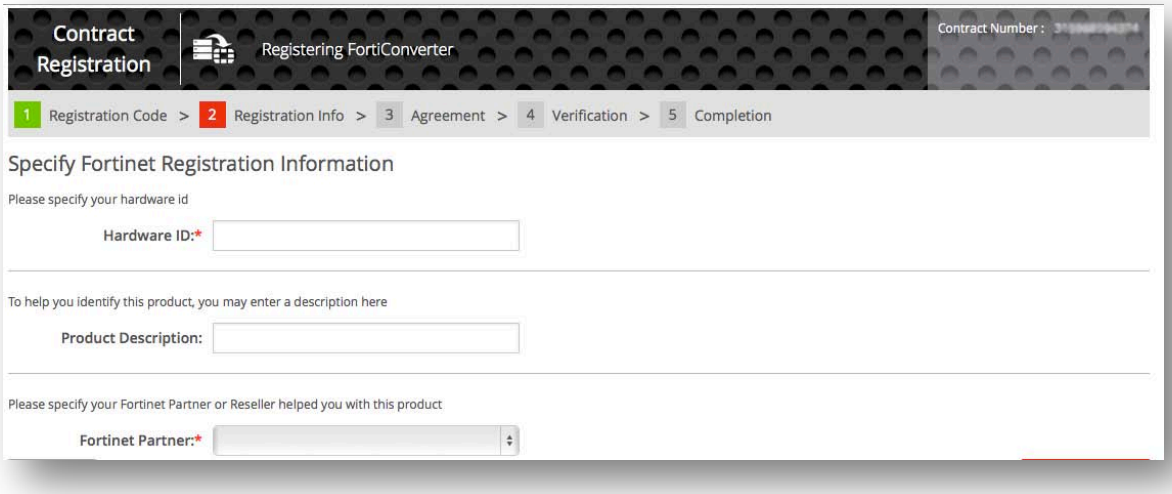
2. Then select the License option from the menu bar

3. This screen now displays your unique Machine Code used during the license process.

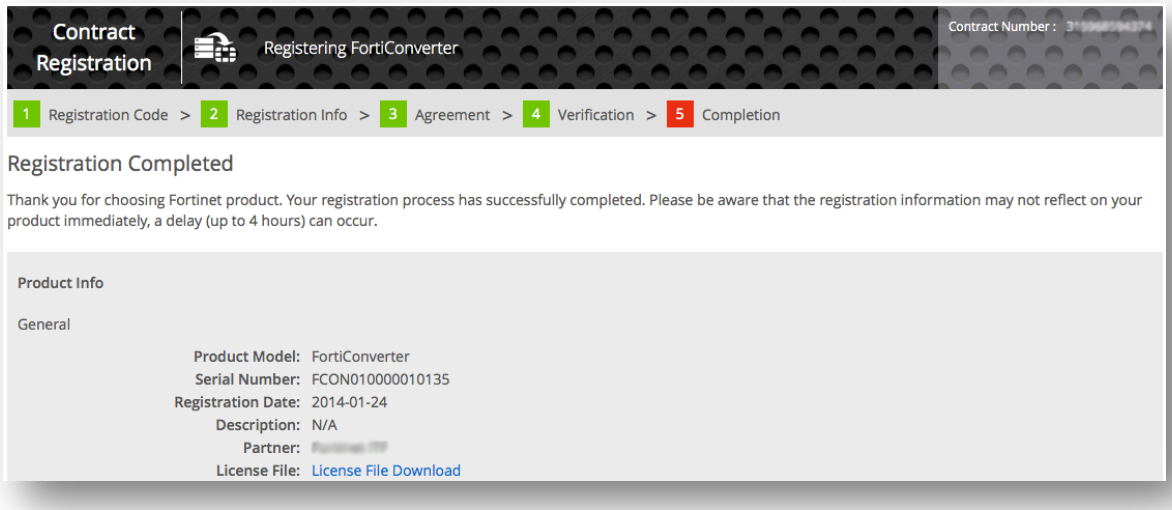
3. Once you have purchased a license, you can sign in to https://support.fortinet.com to download the license file. You will need the machine code obtained in step 3 to link this license file to your machine. To purchase a license, use your usual Fortinet sales channel. The required SKU is provided in the introduction to this document. Registration uses a simple four step wizard and is common to many Fortinet products.



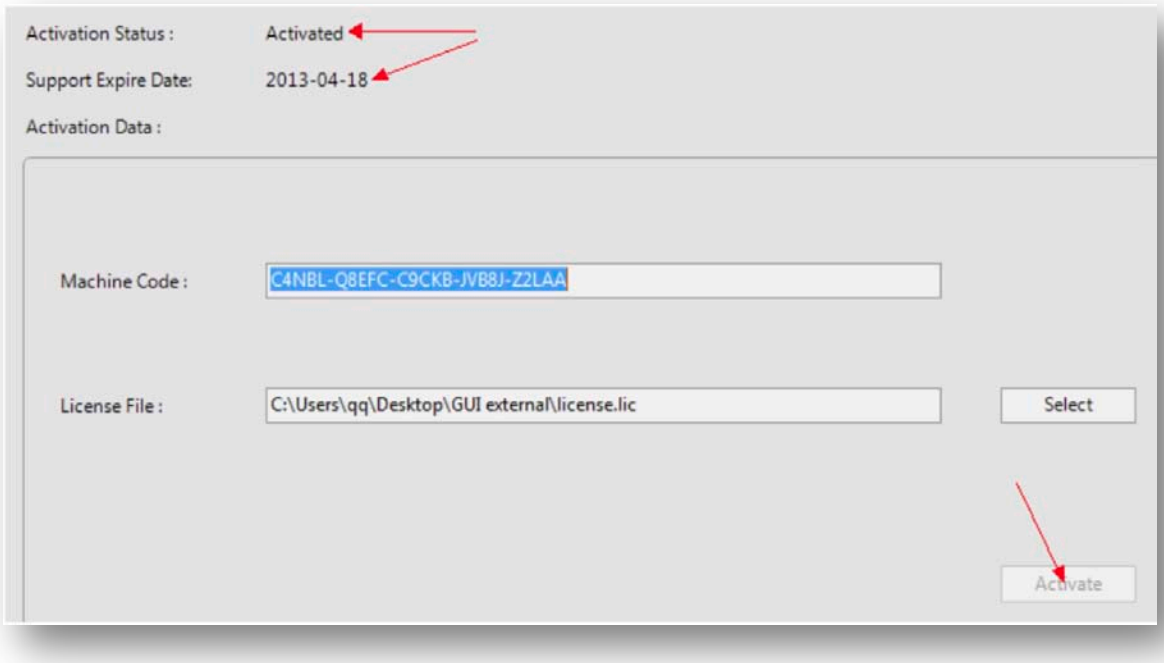
4. Step 2 of the registration wizard requires the Machine Code tfrom the FortiConverter license panel to be entered as the Hardware ID.



5. After agreeing to the license terms the final screen, step 5, allows you to download the license file. It is this file that then needs to be uploaded in to FortiConverter to complete the license activation process.



6. FortiConverter will validate the license file and update the activation status. Your license will be valid for all FortiConverter software until the License Expire Date shown.



Upgrading to a New Version

There is no requirement to remove previous versions of FortiConverter before updating to the latest available release.

Getting Ready for Conversion

Check Point Configuration File

Check Point conversion requires two files:

1. Object definition file (‘objects_5_0.c’ or 'objects.c')
2. Policy and rule definition file (‘*.w’ or ‘rulebases_5_0.fws’)
3. [Optional] route information

4. [Optional] user and user groups file (fwauth.NDBx)

Object Definition File:

This file contains the object definition for the Check Point Firewall. The file name is objects.C (Check Point 4.x) or objects_5_0.C (Check Point NG/NGX).

Policy and Rule Definition File:

This file contains the policy or rule definition for the Check Point Firewall. The file name is <rule>.W (default Standard.W). or rulebases_5_0.fws
You can get those files in the directory of "[SmartCenter]\fw1\conf\".

Route Information:

In order to correctly interpret the network topology being converted, you can provide routing information in addition to the available in the configuration file. This information should be provided as a simple TXT file. You can use the 'route print' command to get the information required to create the route file. There are codes in the output that tell you if it is a directly connected interface, a host route, a network route, and so forth. The output varies depending on the platform.

Cisco Configuration File

Configuration File:
Run the "show running-config" command in the admin console of the Cisco device.
Copy the output content and paste in a TXT file.

Juniper Configuration File

Get configuration file from WebUI:
Configuration file can be obtained from the WebUI: Configuration -> Update -> ConfigFile

Get configuration file from CLI:
Run the "get conf" command in the admin console of the Juniper device.
Copy the output content and paste in a TXT file.

SonicWall Configuration File

Configuration File (*.exp):

Configuration file can be obtained from the WebUI:

System->Settings->Export Settings

Conversion Caveats

General

For some of cases, where interfaces/addresses and service match completely, NAT will be automatically merged into the policy.

All polices with a number starting at 100000 are pure NAT policies that must be manually merged, and always placed at the bottom below all security policies.

When selecting a NAT item, FortiConverter will calculate all correlated and listed policies, for the user to manually apply NAT to security policies.

This will be automated in a future release .

Check Point

Interface command "allow access" is not supported by Check Point. The default is to enable all services for interface.

Interface "Lead to Internet" option is equal to the default gateway route.

When converting Check Point VPN configuration, the "Lead to Internet" interface will be referred as the VPN policy's destination interface. If you changed the default gateway route's interface with the wizard, you may need to update the VPN policy configuration manually.

Time schedule

FortiConverter supports these three types: "by day in month", "by day in week", "none". ”By day in month" will be converted to the FortiOS “once” schedule. ”By day in week" and "none" will be converted to the FortiOS “recur” schedule.

Assign the year range for Check Point "by day in month" time objects. If the specific day does not exist for certain month, FortiConverter will not generate the “once” schedule.

For example, if you configured a Check Point "by day in month" time object with the following parameters:

1. For each year
2. Month: Jan/March/Sept.
3. Day: 1, 5, 31
4. Start and end time: 0:00 to 10:00

If user had assigned a year range value of 1 via the wizard, and had got current year value 2013 from the local PC that ran the wizard, the output content for FortiOS will be:

Once Schedule list:

From 0:00 Jan/1/2013 To 10:00 Jan/1/2013
From 0:00 Jan/5/2013 To 10:00 Jan/5/2013
From 0:00 Jan/31/2013 To 10:00 Jan/31/2013
From 0:00 March/1/2013 To 10:00 March/1/2013
From 0:00 March/5/2013 To 10:00 March/5/2013
From 0:00 March/31/2013 To 10:00 March/31/2013
From 0:00 Sept./1/2013 To 10:00 Sept./1/2013
From 0:00 Sept./5/2013 To 10:00 Sept./5/2013

Since Sept. 31 does not exist, FortiConverter will not add it to the schedule.

Check Point supports a firewall rule action with "Client Auth" option. This option will be converted to the FortiOS “user-identity” policy with an “accept” action.

The static NAT object for Check Point has a 1-to-1 IP mapping relationship; this transform action should be applied to bi-direction traffic. After converting to FortiOS source NAT policy, the policy with IP pool is not restricted to a 1-to-1 IP mapping relationship.

Check Point VPN is not configured within the firewall rule. After converting to FortiOS configuration, FortiConverter will generate several VPN policies from "Intranet" interfaces to "Lead to Internet" interface.

Juniper

Interface names leading with "vlan" will be recognized as logical interfaces.

Juniper ScreenOS configurations that already have NAT configured inside a policy will be automatically converted. NAT fine-tuning is not required.

Cisco

A Cisco “object-group” contains two types of services. Because FortiOS service contains both source and destination port definitions for traffic, only "service-object" can be converted to FortiOS services directly. ”Port-object" cannot be converted directly. FortiConverter will generate FortiOS service objects from ACL's protocol and source / destination services configuration.

Cisco IPsec VPN phase 1 ISAKMP supports three methods: "pre-share", "rsa-sig" and "dsa-sig". FortiOS only supports the first two. Cisco "dsa-sig" will be translated to "rsasig".

If the Cisco ISAKMP has more than one method defined in the configuration, assign the method for each VPN connection via the wizard. Cisco EZVPN configuration will be converted to FortiOS VPN policies with from “Intranet” interfaces, to interface which is assigned by VPN crypto map interface command.

SonicWall

Because FortiOS does not support special characters like ‘#’, ‘(’ and ‘)’, we use these characters ‘*’, ‘[’ and ‘]’ to replace them.

For example, an address book with the name “SNWL #1” will be translated to “SNWL *1”. A service book with the name "Citrix TCP (Session Reliability)” will be translated to "Citrix TCP [Session Reliability]".

FortiOS does not support MAC configuration for the address book, so the related address book objects cannot be converted.

The default address book “Any” represents all IP address for a SonicWall firewall. FortiConverter will generate an address book “Any” for FortiOS.

A FortiOS address/service group object should be configured with at least one member. If a SonicWall configuration contains an empty address/service group object, address “Address_Null” or service “Service_Null” will be generated and referred by the empty address/service group.

There is small difference between SonicWall and FortiOS schedule groups. SonicWall schedule groups can include only one “onetime” schedule and multiple “recur” schedules. The “onetime” schedule is an implicit object that can be embedded into the schedule group. Because FortiOS does not support this implicit attribution, every object (onetime or recur) that

can be referred by a schedule group needs to be defined explicitly. This difference leads to some auto-generated “onetime” schedules within the configuration output.

FortiOS “onetime” or “recur” time schedule cannot support a time value “24:00” (equal to the next day’s 00:00). When converting SonicWall time schedule “M 00:00 to 24:00”, FortiConverter sets the end time with “00:00”.

Local user’s password is a cipher string. FortiConverter sets it as “123456”.

Nested user groups are not supported. For example, if there “group1” belongs to “group2”, “group2”, will be empty after conversion.

Conversion of tunnel routes is not supported (static route with the next hop tunnel interface).

IPSec VPN/tunnel conversion is not supported.

Because FortiOS configures NAT rules within a policy module, each SonicWall NAT rule will be converted to one policy entry. If the NAT rule’s status is enabled, then the converted policy status is also set to enabled. The converted policy ID for NAT rule starts from 100001. The regular firewall policy ID starts from 10000.

For source NAT rules, FortiConverter will create a new IP pool object for the FortiOS policy’s source address.

For example, a SonicWall source NAT rule looks like this:

Org Src	Tran Src	Org Dest	Tran Dest	Org Serv	Tran Serv
All Interface IP	X2 IP	Any	Original	Any	Original

After converting to the FortiOS configuration, a new IP pool object with name “ippool-X2 IP” will be created. FortiConverter adds a prefix “ippool-” before the translated source address book “X2 IP”.

For destination NAT rules, FortiConverter creates a new VIP object for the FortiOS policy’s destination address.

For example, a SonicWall destination NAT rule looks like this:

Org Src	Tran Src	Org Dest	Tran Dest	Org Serv	Tran Serv
LAN Subnets	Original	WoW Static IP	X0 IP	SSLVPN	Original

After converting to a FortiOS configuration, a new VIP object with name “vip-X0 IP” will be created. FortiConverter adds a prefix “vip-” before the translated destination address book “X0 IP”.

For destination NAT configuration, FortiOS destination NAT only supports VIP and VIP group. The VIP object is restricted to a 1-to-1 address and port mapping between the external and internal network.

For example, a SonicWall source and destination NAT policy looks like this:

Org Src	Tran Src	Org Dest	Tran Dest	Org Serv	Tran Serv
test_1112_grp	test_11_gw	test_12_gw	test_1211_grp	Echo	Original

Address book “test_12_gw” only contains one IP address, but address group “test_1211_grp” contain two address members “test_11_gw” and “test_12_gw”.

This NAT rule will translate an IP packet’s destination address from address book “test_12_gw” to address group “test_1211_grp”. FortiOS cannot generate a VIP object for this

NAT rule, because the address book “test_12_gw” and the address group “test_1211_grp” contain different counts of IP addresses.

Issues

The resolved issues listed below do not include every bug that has been corrected with this release. For inquires about a particular bug, please contact the support email alias fconvert_feedback@fortinet.com

Table 1: Known/Resolved ... issues.

Bug ID	Description
224085	Incorrect conversion statistics
224245	HTML conversion pages don’t work for trial version
224246	CHECKPOINT: Wrong conversion caused by malformed configuration
224249	CISCO: Unconverted cisco configuration output is not reported
224251	CHECKPOINT: Trial mode of Provider-1 not working
224257	Lack of cross reference for firewall objects
224259	Go to output button incorrectly linked
224256	Error on IP ranges from address book